**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

CRYPTOPEAK SOLUTIONS, LLC,	
Plaintiff,	Case No. 2:15-cv-1731
v.	**PATENT CASE**
COSTCO WHOLESALE CORP.,	**JURY TRIAL DEMANDED**
Defendant.	
MACYS.COM, INC.	Case No. 2:15-cv-1738
SEARS HOLDINGS MANAGEMENT CORPORATION, *et al.*	Case No. 2:15-cv-1742
WILLIAMS-SONOMA, INC.	Case No. 2:15-cv-1750
ALLY FINANCIAL INC., *et al.*	Case No. 2:15-cv-1787
EXPEDIA, INC., *et al.*	Case No. 2:15-cv-1791
YAHOO! INC., *et al.*	Case No. 2:15-cv-1804

**PLAINTIFF CRYPTOPEAK'S RESPONSE IN OPPOSITION TO
DEFENDANTS' MOTIONS TO DISMISS UNDER FED. R. CIV. P. 12(B)(6)**

Craig Tadlock
State Bar No. 00791766
John J. Harvey, Jr.
State Bar No. 09179770
Keith Smiley
State Bar No. 24067869
TADLOCK LAW FIRM PLLC
2701 Dallas Parkway, Suite 360
Plano, Texas 75093
903-730-6789
craig@tadlocklawfirm.com
john@tadlocklawfirm.com
keith@tadlocklawfirm.com

*Attorneys for Plaintiff
CryptoPeak Solutions, LLC*

1

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES:

Plaintiff CryptoPeak Solutions, LLC ("Plaintiff" or "CryptoPeak") files this Response in Opposition to the Motions to Dismiss Under Fed. R. Civ. P. 12(b)(6), filed in the above-captioned cases by Defendants in the above-captioned cases Costco Wholesale Corp.; Macys.com Inc.; Sears Holdings Management Corporation, *et al.*; Williams-Sonoma, Inc.; Ally Financial Inc.*, et al.*; Expedia, Inc., *et al.*; and Yahoo! Inc.*, et al.* (collectively referred to as the "Moving Defendants"), and in support thereof shows the Court as follows:

INTRODUCTION

The patent-in-suit, U.S. Patent No. 6,202,150 (the "'150 Patent"), filed in 1997 in much earlier days of the Internet, introduced a new and inventive method for secure computing over a network using techniques from the field of cryptology. The inventors are two Ph.D. computer scientists who are esteemed in the field.

Very generally, the invention of the '150 Patent solves problems in secure computing related to public-private key encryption systems and key escrow. This is done by providing an efficient and secure method by which secure, encrypted connections can be established – for example, a server (such as the server of a bank or online retailer) can send a secure, encrypted communication to a client (such as the computer of a person using online banking or making an online purchase), and the client will be able to utilize the encrypted communication with confidence, even though the communication was generated using the server's private key but the client does not have access to the private key (which of course would cause serious security issues). The server utilizes a proof that provides confidence to the client that the public key it received to decrypt the communication is genuine. The benefits of this method include an enhanced, more secure connection between the server and the client, and it eliminates any need for third party key escrow authorities (which substantially reduces costs, improves security, and enhances speed).

More recently, the inventive methods of the '150 Patent have become widely utilized for secure computing by many types of companies, including online banks, brokerages, ecommerce retailers, Internet media companies, and travel-related companies. For the defendants in the CryptoPeak cases, this infringement occurs via their extensive use of a standardized protocol that has become the proverbial gold standard for secure online communications.

The Moving Defendants assert two grounds for dismissal in their Motions to Dismiss. One, the Moving Defendants assert that the Potentially Asserted Claims[1] of the '150 Patent are invalid as indefinite *per se* on "mixed subject matter" grounds, because they contain the phrase "A method and apparatus for …" in the preamble, even though the substance of the claims exclusively comprises method steps. Two, the Moving Defendants assert that the Potentially Asserted Claims are invalid because they are subject matter ineligible under 35 U.S.C. § 101.[2] Neither ground supports dismissal.

As for the "mixed subject matter" grounds, in substance, the claims are clearly ***method*** claims that require action, and the Court must look to the substance of the claims for patent eligibility purposes. The recitation of some physical structure in connection with method claims does not invalidate those claims. Case law from the Federal Circuit and this District, including the local case of *Oasis Research, LLC v. AT&T Corp.*, 2012 WL 602202 (E.D. Tex. Feb. 23, 2012) (Mazzant, J.) (attached as Ex. A), demonstrates that the Potentially Asserted Claims are valid.

As for the "subject matter eligibility" grounds, the '150 Patent easily passes muster because it claims a quintessential "solution [that] is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks" and is therefore

---

[1] As defined in CryptoPeak's Complaints, Claims 1, 2, 3, 4 and 17 of the "'150 Patent."

[2] The Ally defendant group asserts only the second grounds based on subject matter ineligibility. The Ally defendant group does not assert "mixed subject matter" grounds.

subject matter eligible. *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257 (Fed. Cir. 2014).

PROCEDURAL BACKGROUND

1.   On July 17, 2015, CryptoPeak filed a first set of cases (the "First Wave Cases") alleging infringement of the '150 Patent, which is entitled Auto-Escrowable and Auto-Certifiable Cryptosystems." *See, e.g.*, Dkt. No. 1 in Case No. 2:15-cv-1284. Many of these cases have been resolved, and the remaining defendants in the First Wave Cases have been consolidated for pretrial purposes (excluding venue) into Lead Case No. 2:15-cv-1284. This Lead Case is set for a scheduling conference on March 15, 2016.

2.   Several of the defendants in the First Wave Cases filed Motions to Dismiss. (*See, e.g.,* Dkt. No. 18 in Case No. 2:15-cv-1288.) The grounds for these Motions are that CryptoPeak's Amended Complaints must be dismissed as a matter of law for failure to state a claim, on the grounds that the Potentially Asserted Claims (*i.e.*, Claims 1, 2, 3, 4 and 17) of the '150 Patent are invalid for reciting "mixed subject matter" under *IPXL Holdings, LLC v. Amazon.com, Inc.*, 430 F.3d 1377 (Fed. Cir. 2005). These "mixed subject matter" motions are fully briefed and pending before the Court.

3.   On November 9, 20 and 25, 2015, CryptoPeak filed additional patent infringement actions, also asserting infringement of the '150 Patent (the "Second Wave Cases"). All of the Moving Defendants are defendants in the Second Wave Cases. All defendants in the Second Wave Cases have appeared, and the Second Wave Cases are ready for a scheduling conference.

4.   Some of the defendants in the Second Wave Cases filed "mixed subject matter" motions to dismiss. CryptoPeak has responded to those motions, which are identical in substance to the "mixed subject matter" motions filed by certain defendants in the First Wave Cases.

5.   The Moving Defendants here filed Rule 12(b)(6) motions to dismiss based on two grounds – one, the same "mixed subject matter" grounds previously asserted by several defendants in the related cases; and two, "subject matter ineligibility" grounds under 35 U.S.C. § 101.[3]

6.   Not one of the defendants in the First Wave Cases asserted 101-based "subject matter ineligibility" grounds as a basis for a motion to dismiss.[4] This is not surprising, because as previously discussed, the '150 Patent claims a quintessential "solution [that] is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks" and is therefore subject matter eligible under *DDR Holdings* and its progeny.

FACTUAL BACKGROUND

7.   The '150 Patent generally relates to the field of cryptography/cryptology and secure transmissions and transactions over a network. It is entitled "Auto-Escrowable and Auto-Certifiable Cryptosystems." (*See, e.g.*, the '150 Patent at Dkt. No. 1-1 in Case No. 2:15-cv-1731.) Generally, the Accused Instrumentalities in the Complaints are websites that utilize Elliptic Curve Cryptography ("ECC") Cipher Suites for the Transport Layer Security ("TLS") protocol; for example, the Accused Instrumentality identified in the Complaint for Defendant Costco is its website www.costco.com. (*See, e.g.,* Dkt. No. 1 in Case No. 2:15-cv-1731 (the "Costco Complaint") at ¶ 21.)

8.   The application that resulted in the '150 Patent was filed on May 28, 1997. The inventors are Dr. Adam L. Young and Dr. M. M. ("Moti") Yung. Both Dr. Yung and Dr. Young are noted and accomplished experts in the field of the invention of the '150 Patent, which is

---

[3] As previously noted, the motion filed by the Ally defendant group asserts only "subject matter ineligibility" grounds. *See* Dkt. No. 12 in Case No. 2:15-cv-1787.

[4] And there were 29 defendant groups in the First Wave Cases, represented by some of the biggest law firms and most clever patent defense lawyers in the United States.

cryptology.   In short, cryptology is the science and practice of designing computation and communication systems which are secure in the presence of adversaries. (*See* the website of the International Association for Cryptologic Research, https://www.iacr.org/.) (*See, e.g.,* Costco Complaint at ¶ 12.)

9.   Dr. Moti Yung obtained his Ph.D. in Computer Science in 1988 at Columbia University. His professional career includes research and technical work for IBM, RSA Security (now a division of EMC), and Google. He has been an adjunct professor for many years at Columbia University, serving on Ph.D. committees and advising more than 60 Ph.D. students. He is an author or co-author of more than 300 refereed abstracts and journal papers, including several in collaboration with Dr. Young. He is an inventor on dozens of issued U.S. patents. He is a Fellow of the ACM (Association for Computing Machinery), the IACR (International Association for Cryptologic Research), and the IEEE (Institute of Electrical and Electronics Engineers). (*See, e.g.,* Costco Complaint at ¶ 13.)

10.   Dr. Adam Young obtained his Ph.D. in Computer Science in 2002 at Columbia University. His professional career includes research and technical work for Lucent, Lockheed Martin, MITRE Corporation, and Bloomberg. He has been a guest lecturer at NYU and Rensselaer Polytechnic Institute. He is an author or co-author of more than three dozen papers and journal articles, including several with Dr. Yung. He is an inventor on at least 8 issued U.S. patents. (*See, e.g.,* Costco Complaint at ¶ 14.)

11.   Dr. Yung and Dr. Young also co-authored a book published in 2004, entitled "Malicious Cryptography: Exposing Cryptovirology." (*See, e.g.,* Costco Complaint at ¶ 15.)

12.   The '150 Patent is a prominent patent in its field. It has been forward-cited as prior art in connection with the examination of at least 20 subsequently-issued U.S. patents, including

patents originally assigned to such prominent technology companies as Microsoft, HP, General Instrument, Ricoh and Sungard. (*See, e.g.,* Costco Complaint at ¶ 16.)

13.   Moreover, the invention of the '150 Patent was sufficiently prominent that an article, entitled "Auto-Recoverable Auto-Certifiable Cryptosystems," which is related to the subject matter of the '150 Patent, was published and presented by Drs. Yung and Young in connection with the prestigious EUROCRYPT '98 conference in Espoo, Finland. EUROCRYPT is an annual conference that has been held since 1982, and it is one of the IACR's three flagship conferences, along with CRYPTO and ASIACRYPT. (*See, e.g.,* Costco Complaint at ¶ 17.) This published article is attached as Exhibit B hereto, as it is specifically referenced in CryptoPeak's Complaint.

14.   In its Complaints against each of the Moving Defendants, CryptoPeak specifically alleges that each of the Potentially Asserted claims is a ***method*** claim comprising certain steps that must be performed in order for infringement to occur. (*See, e.g.,* Costco Complaint at ¶ 19) ("Notwithstanding that they generically recite the existence of 'apparatus' in their preambles, each of the Potentially Asserted Claims is a method claim comprising certain steps that must be performed in order for infringement to occur.") These allegations address the Moving Defendants' "mixed subject matter" arguments.

ARGUMENT AND AUTHORITIES

A.   Legal Standards for Motions to Dismiss Under Rule 12(b)(6)

The legal standard for a Motion to Dismiss under Rule 12(b)(6) is well known to this Court. On a 12(b)(6) Motion, the Court "accepts all well pleaded facts as true, viewing them in the light most favorable to the plaintiff." *Guidry v. Am. Pub. Life Ins. Co.*, 512 F.3d 177, 180 (5th Cir. 2007). The Court must accept all factual allegations in the complaint as true and draw all

reasonable inferences in favor of the non-movant. *Erickson v. Pardus,* 551 U.S. 89, 93-94 (2007);

Bowlby v. City of Aberdeen, 681 F.3d 215, 218 (5th Cir. 2012).

The court may consider "the complaint, any documents attached to the complaint, and any

documents attached to the motion to dismiss that are central to the claim and referenced by the

complaint." *Lone Star Fund V (U.S.) L.P. v. Barclays Bank PLC*, 594 F.3d 383, 387 (5th Cir.

2010). The court must then decide whether those facts state a claim for relief that is plausible on

its face. *Bowlby*, 681 F.3d at 217. "A claim has facial plausibility when the pleaded factual content

allows the court to draw the reasonable inference that the defendant is liable for the misconduct

alleged." *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009)).

Issued patents are presumed valid, and the accused infringer bears the burden of proving

invalidity by clear and convincing evidence. *See* 35 U.S.C. § 282, *Commil USA, LLC v. Cisco

Sys.*, 1351 S. Ct. 1920, 1929 (2015). Close questions of indefiniteness "are properly resolved in

favor of the patentee." *Datamize, LLC v. Plumtree Software, Inc.*, 417 F.3d 1342, 1348 (Fed. Cir.

2005); *SFA Sys., LLC v. 1-800-Flowers.com, Inc.*, 940 F. Supp. 2d 433, 453 (E.D. Tex. 2013)

(Davis, J.).

B.   The Motions to Dismiss on "Mixed Subject Matter" Grounds Should Be Denied Because the Potentially Asserted Claims Are Proper "Method" Claims and not Improper "Mixed Subject Matter" Claims, and for a Number of Other Reasons

As previously mentioned, the "mixed subject matter" grounds for dismissal have been fully

briefed in related cases and are pending before the Court. *E.g., CryptoPeak Solutions, LLC v. AOS,

Inc. d/b/a Trading Block*, Case No. 2:15-cv-1288, Dkt. Nos. 18 (Motion), 19 (Response), 20

(Reply), and 21 (Sur-Reply).[5]   The Moving Defendants may articulate these grounds slightly

differently, but their arguments are substantively identical to the earlier-filed motions.

---

[5] This case has subsequently been consolidated into Lead Case No. 2:15-cv-1284; however, all briefing was done prior to consolidation, and all docket numbers are from the member -1288 case.

In its briefing in the earlier related cases, CryptoPeak demonstrates that motions to dismiss on "mixed subject matter" grounds should be denied because the Potentially Asserted Claims are proper "method" claims and not improper "mixed subject matter" claims, and are therefore valid claims under controlling case law. Although Cryptopeak does not want to unduly burden the Court with unnecessary briefing, it may be helpful to recap CryptoPeak's arguments here for completeness.

The Motions to Dismiss on "mixed subject matter" grounds should be denied for a number of reasons:

1.   The Moving Defendants primarily contend that the Potentially Asserted Claims are invalid as indefinite *per se* because they contain the phrase "A method and apparatus for …" in the preamble. This is not the law. Instead, the Court must look to the substance of the claims at issue, and the substance demonstrates conclusively that these are ***method*** claims.

The structure of the Potentially Asserted Claims of the '150 Patent, using Claim 1 as an example, is as follows (key elements for this analysis in bold/italics/underline):

Preamble (signaling **method** steps)	***A method and apparatus for*** generating public keys and a proof that the keys were generated by a specific algorithm ***comprising the steps of***:
Body of Claim / Limitations (all **method** steps)	***the user's system generating a random string*** of bits based on system parameters; ***the user running a key generation algorithm*** to get a secret key and public key using the random string and public parameters; ***the user constructing a proof*** being a string of bits whose public availability does not compromise the secret key, but at the same time said proof provides confidence to at least one of a plurality of other entities that said public key was generated properly by the specified algorithm, and wherein said confidence is gained without having access to any portion of said public key.

"Regardless of what statutory category ('process, machine, manufacture, or composition of matter,' 35 U.S.C. § 101) a claim's language is crafted to literally invoke, we look to the underlying invention for patent-eligibility purposes." *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1374 (Fed. Cir. 2011); *accord CLS Bank Int'l v. Alice Corp. Pty. Ltd.*, 717 F.3d 1269, 1288 (Fed. Cir. 2013), *aff'd*, 134 S. Ct. 2347 (2014) ("[W]e must look past drafting formalities and let the true substance of the claim guide our analysis."). Courts have applied this rule in numerous cases, including *CyberSource* and *CLS Bank*, to treat claims as method claims even though they were nominally described in the preamble as a "system" or other physical device. *E.g., CyberSource*, 654 F.3d at 1374-75; *CLS Bank*, 717 F.3d at 1288; *DietGoal Innovations LLC v. Bravo Media LLC*, 33 F. Supp. 3d 271 (S.D.N.Y. 2014); *Oasis*, 2012 WL 602202. The Moving Defendants uniformly ignore this requirement.

In *CyberSource*, despite the fact that the preamble of the claim at issue described "[a] computer readable medium," the Federal Circuit found that "it is clear that the invention underlying both claims 2 and 3 is a ***method*** for detecting credit card fraud, not a manufacture for storing computer-readable information." *CyberSource*, 654 F.3d at 1374 (emphasis added) (citing *In re Abele*, 684 F.2d 902 (CCPA 1982)).

Similarly, in *CLS Bank*, the Federal Circuit held that a patent claim nominally reciting a "computer readable storage medium" was a method claim in substance and should be treated as such:

> ***Claim 39 thus nominally recites as its subject matter a physical device – a "computer readable storage medium"*** … But under § 101 ***we must look past drafting formalities and let the true substance of the claim guide our analysis***. Here, although the claim's preamble appears to invoke a physical object, the claim term "computer readable storage medium" is stated in broad and functional terms – incidental to the claim – and every substantive limitation presented in the body of the claim (as well as in dependent claims 40 and 41) pertains to the method steps of the program code "embodied in the medium." Therefore, claim 39 is not "truly

drawn to a specific computer readable medium, rather than to the underlying method" … Alice's "computer readable medium claims" are thus equivalent to the methods they recite for § 101 purposes. ***In other words, they are merely method claims*** in the guise of a device[.]

CLS Bank, 717 F.3d at 1288 (emphasis added).

In *DietGoal*, the preamble of two claims at issue described "[a] system of computerized meal planning…" *DietGoal*, 33 F. Supp. 3d at 274. The plaintiff argued that the patent in suit claimed patentable "machine." *Id.* at 282 n.5. The court analyzed the substance of the claims, however, and concluded that they were in substance "process" or "method" claims:

"However, the '516 Patent does not claim a computer, or a machine of any type, as its invention. Rather, the independent claims of the '516 Patent recite a 'system' and a 'method' of computerized meal planning, which is to be implemented on an existing general purpose computer. ***These claims clearly contemplate a process, not a machine***."

Id. (emphasis added) (citing 35 U.S.C. § 100 ("the term 'process' within the meaning of the Patent Act 'means a process, art or method …'")).

In *Oasis*, which will be discussed at more length below, Judge Mazzant held that a claim nominally described as a "system" in the preamble ("An online computer system …") was in substance a method claim, because the body of the claim exclusively contained method/action steps such as "providing," "establishing," and "requesting." *Oasis*, 2012 WL 602202. Importantly, Judge Mazzant's analysis was in the context of the same doctrine that the Moving Defendants invoke here – that is, a contention that the claim at issue was invalid as indefinite under the "mixed subject matter" doctrine. *Id.*

2.   Evaluating the substance of the claims as is required, the Potentially Asserted Claims of the '150 Patent are clearly ***method*** claims. First, the preamble of the claims ends with the phrase "comprising the steps of," which definitively signals that the steps of a patented method are to follow. Then, the body of the claims is comprised solely of ***method*** steps that must be

performed for infringement to occur, that is, "the user's system generating …", "the user running a key generation algorithm …", and "the user constructing a proof…"

Remarkably, the Moving Defendants contend that the inclusion of the phrases "the user's system" and "the user" in these claim elements improperly injects "system" elements into these claim terms. Not surprisingly, the Federal Circuit has repeatedly held (including in the *IPXL* case itself) that claim elements written exactly like those at issue here are indeed ***method*** steps. *E.g., H-W Tech., L.C. v. Overstock.com, Inc.*, 758 F.3d 1329, 1336 (Fed. Cir. 2014) ("wherein said user completes" and "wherein said user selects" are method steps); *In re Katz Interactive Call Processing Patent Litigation*, 639 F.3d 1303, 1318 (Fed. Cir. 2011) ("said certain of said individual callers digitally enter data" is a method step); *IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377, 1384 (Fed. Cir. 2005) ("the user uses the input means" is a method step).

Moreover, the recitation of an apparatus in a method claim typically aids in understanding of the claim, and such method claims are therefore not invalid for indefiniteness solely because they might include recitations of an apparatus. *See, e.g., Collaboration Properties, Inc. v. Tandberg ASA*, 2006 WL 1752140 at **2-6 (N.D. Cal. June 23, 2006) (attached as Ex. C); *accord* O'Neill and Guzniczak, *Treatment of "Hybrid" Claims in the Courts*, Bloomberg Law Reports – Intellectual Property, Vol. 5, No. 27 (2011) (available at http://www.fitzpatrickcella.com/DB6EDC/assets/files/News/oneill%20guzniczak%20treatment%20of%20hybrid%20claims%20(2).pdf) (attached as Ex. D). This is true even if the recitation of physical structure is in the preamble. *Microprocessor Enhancement Corp. v. Texas Instruments, Inc.*, 520 F.3d 1367, 1375 (Fed. Cir. 2008) ("Method claim preambles often recite the physical structures of a system in which the claimed method is practiced[.]").

3.   *IPXL v. Amazon* does not set forth a *per se* rule that every patent claim that contains

the terms "method" and "apparatus" is invalid. Rather, this case has a very narrow holding, and

there are many judicial rejections of parties' attempts to use the *IPXL* defense in cases addressing

so-called "mixed subject matter" claims after *IPXL* was decided. *See, e.g., Technology Patents*

LLC v. Deutsche Telekom AG, 774 F.Supp.2d 732 (D. Md. 2010); *see also SFA Sys., LLC v. 1-*

800-Flowers.com, Inc., 940 F. Supp. 2d 433, 453-455 (E.D. Tex. 2013) (Davis, J.). As the Federal

Circuit held in the *Microprocessor Enhancement* case, which was decided three years after *IPXL*

v. Amazon, "The conclusion of *IPXL Holdings* was based on the lack of clarity as to when the

mixed subject matter claim would be infringed…. There is no similar ambiguity [here]."

Microprocessor Enhancement, 520 F.3d at 1374-75. Likewise, there is no lack of clarity in the

Potentially Asserted Claims that they are infringed only when the method steps are practiced.

Judge Davis pointed out the limitations of *IPXL* in his discussion in the *SFA Systems* case,

where he found that the claims at issue were not invalid as "mixed subject matter" claims under

IPXL. As Judge Davis stated, "the claims in those cases [*IPXL* and its progeny] suffered from a

true ambiguity as to whether the claims require building a product or performing a method. In

particular, those cases involved apparatus claims incorporating steps where a user acts *upon the*

system." *SFA Sys.*, 940 F. Supp. 2d at 455 (emphasis in original). Judge Davis in *SFA Systems*

found that for those claims, "there is no uncertainty about when infringement would occur – it

plainly occurs when a system is created that can perform the claimed function." Analogously here,

there is no uncertainty about when infringement would occur – it plainly occurs when the method

steps set forth in the Potentially Asserted Claims are performed.

4.   Alternatively, to the extent the Court believes there is any lack of clarity, the

determination of whether one skilled in the art would understand the claims would involve fact

issues that could not be determined on a motion to dismiss. This is a claim construction issue.

CryptoPeak has the right and if necessary requests the ability to submit evidence on these fact

issues, including without limitation expert testimony and potentially inventor testimony, on this

issue, which cannot be done on a motion to dismiss. Moreover, the patent in suit is presumed to

be valid, and the standard of proof for invalidity is clear and convincing evidence. *Commil USA,*

LLC v. Cisco Sys., 1351 S. Ct. at 1929.

      5.   Along the same lines, there is no case law that the word "apparatus" in the preamble

is somehow a "magic word" that requires invalidation without looking further at the claims.[6]

Instead, the word "apparatus" in the preamble and the references to "the user's system" or the

"user" in claims that are plainly method claims in substance, simply reflects the commonsense fact

that every method must be performed by ***some*** person and/or by ***some*** physical thing. Moreover,

CryptoPeak has specifically pleaded that the Potentially Asserted Claims are all ***method*** claims,

and to the extent this is a fact issue, the facts pleaded by CryptoPeak must be taken as true. This

is not a matter of CryptoPeak trying to rewrite the claims or have the Court correct them, as the

Moving Defendants erroneously contend, but rather a straightforward analysis of the substance of

the Potentially Asserted Claims.

      And even though the preamble of each Potentially Asserted Claim includes the word

"apparatus," (1) the preamble is not limiting, and (2) in the exceptions where a preamble may be

---

[6] The Expedia Defendants (and other clients of the same law firm) erroneously cite *Ex Parte Penke*, 2008 WL 4768089 (BPAI Oct. 31, 2008) for the proposition that the Board invalidated a claim solely based on a preamble reciting a "marking system and process." *See* Dkt. No. 19, Case No. 2:15-cv-1791, at p. 6. A closer reading of *Ex Parte Penke* reveals that this reading is incorrect. The Board actually reviewed the substance of the claims in finding them indefinite. *Ex Parte Penke*, 2008 WL 4768089 at *2 ("Plainly, claim 28 recites that the structure of the marking system 'comprises in an operative arrangement at least one sensor, a marking station …' Claim 28 further recites a process of using the apparatus. For example, 'said sensor enabled to activate at least one signal including illumination at said collection station' (claim 28). The inclusion of a process of use in an apparatus claim renders the claim indefinite under 35 U.S.C. § 112, second paragraph, for the reasons provided *supra*. [citing *IPXL v. Amazon*]").

treated as limiting, the decision "[w]hether to treat a preamble term as a claim limitation is 'determined on the facts of each case in light of the claim as a whole and the invention described in the patent.'" *American Medical Systems, Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1358-59 (quoting *Storage Tech. Corp. v. Cisco Sys., Inc.*, 329 F.3d 823, 831 (Fed. Cir. 2003)). The Court, of course, cannot determine disputed fact issues on a motion to dismiss.

6.   The recent *Oasis* case in this District is almost directly on point and fully supports CryptoPeak's position. In *Oasis*, the defendants filed a motion for partial summary judgment of indefiniteness against certain claims of the patent in suit under the "mixed subject matter" doctrine. The independent claim at issue read as follows (in relevant part):

Preamble (nominally reciting a **system**, yet signaling **method** steps)	*An online computer system* providing commercial backup services to remote customer computers over the Internet *by performing the following steps*:

Body of Claim / Limitations (reciting **method** steps requiring action)	(a) *providing* at least one remote storage area …;
	
	(b) *establishing* a first online Internet session …;
	
	(c) *allowing* the customer to sign up …;
	
	(d) *establishing* a second online Internet session …;
	
	(e) *requesting* the customer to input …;
	
	(f) *validating* the customer identifier …;
	
	(g) conditioned at least in part on validating step (f), *allowing* the customer to access the remote storage area …, *including the steps of*:
	     (1) *encrypting* backup data …;
	     (2) *transmitting* the encrypted backup data …;
	     (3) *storing* the backup data …

Oasis, 2012 WL 602202 at **2-3.

The defendants in *Oasis* argued that this claim was indefinite for improperly claiming mixed subject matter, relying on *IPXL* and the MPEP provision that the Moving Defendants cite

in their motions, among other things. *Id.* at ** 3-4. The plaintiff countered that this claim was a

method claim as indicated by the performance of a series of steps and, like CryptoPeak here, cited

the *Microprocessor Enhancement* case as support. *Id.* at 3. Notwithstanding the nominal recitation

of a "system" in the preamble, Judge Mazzant squarely rejected defendants' "mixed subject

matter" arguments and denied their motion:

> Claim 1 does not contain both apparatus and method claims. Despite the language
> in the preamble of Claim 1 that refers to an "online computer system providing
> commercial backup services," the language in the claim itself clearly contains
> method steps. "A method claim is composed of a series or sequence of steps, each
> of which should state an operation expressed in the form of the present participle
> ('ing'), as, for example, 'heating…,' 'cooling…,' 'reacting…' Such are sometimes
> referred to as active or action steps." Donald C. Reiley III, et. al., 3 Patent Law
> Fundamentals § 14:41 (2d ed. 2011). The steps in Claim 1 consist of the following
> language: (a) providing …; (b) establishing …; (c) allowing …; (d) establishing …;
> (e) requesting …; (f) validating …; and (g) allowing. The Federal Circuit held in
> *Microprocessor*, "[m]ethod claim preambles often recite the physical structures of
> a system in which the claimed method is practiced." *Microprocessor*, 520 F.3d at
> 1374. Claim 1 is no different, since the preamble recites the structure of a system
> in which the method is practiced.

Id. at *3. The identical rationale applies here – the Potentially Asserted Claims of the '150 Patent

are undoubtedly "method" claims, notwithstanding the nominal presence of the word "apparatus"

in the preamble.

       7.   The BPAI case of *Ex parte Lyell*, 17 U.S.P.Q.2d 1548, 1990 WL 354583 (BPAI

1990), which the Moving Defendants cite, does not support invalidation of the claims of the '150

Patent. *Lyell* is readily distinguishable because the claim at issue there included both system

elements and method steps in the **body** of the claim (as well as nominally reciting both a system

and a method in the preamble).

      The claim at issue in *Lyell* read (in relevant part):

Preamble (nominally reciting a **system** and a **method**)	***An automatic transmission tool in the form of a workstand*** and ***method*** for using same comprising:

Body of Claim / Limitations (**system** elements)	a support means, and [sic] internally splined sleeve …, a threaded adjustment bolt …,
and	and further comprising the steps of
(**method** steps)	1. positioning the output end …, 2. removing the internal components …, 3. repairing and replacing said internal components …, 4. adjusting said internal components.

Ex parte Lyell, 1990 WL 354583 at *1.

Not surprisingly, the Board rejected this claim because it impermissibly purported to claim both an apparatus and a method of using the apparatus in the body of a single claim. *Id.* at **1-6. The situation present in *Lyell* is not present here, however. The substance of the Potentially Asserted Claims of the '150 Patent clearly shows them to be **_method_** claims. Unlike the claim at issue in *Lyell*, the body of the Potentially Asserted Claims at issue here and the limitations expressed therein express **_method_** steps only. Accordingly, *Lyell* is not on point here.

8.   The Moving Defendants do not cite any cases where a claim consisting of method steps is invalidated simply because it includes some recitation of physical structure or apparatus. Instead, the Moving Defendants attempt to rely on "mixed subject matter" cases where the claims at issue are clearly system claims, and the question is whether those system claims improperly contain method steps. These cases apply a different line of case law, and they are off-point.

This type of case is well-known to this Court – the dispute relates to a system/apparatus claim and boils down to whether the claim element at issue (*i.e.*, the purported "method" step) constitutes (a) permissible functional/capability language, or (b) an impermissible method step that requires a person or system to affirmatively perform some designated act. The difference is exemplified by two recent cases before this Court. *Contrast E-Watch Inc. v. Apple Inc.*, 2015 WL

1387947 at **5-6 (E.D. Tex. Mar. 25, 2015) (Payne, J.) ("operation of the input device by the

user" and "movement by the user" are impermissible method steps), *with Core Wireless Licensing*

S.A.R.L. v. LG Electronics, Inc., 2015 WL 6956722 at **12-13 (E.D. Tex. Nov. 9, 2015) (Payne,

J.) ("circuitry operable to send a request" and "circuitry operable to receive" comprise proper

functional/capability language that does not create a "mixed subject matter" problem).

This line of cases does not apply here, because the substance of the Potentially Asserted

Claims describes a method. Judge Mazzant in *Oasis* made precisely this point in holding this line

of cases to be inapplicable, and he expressly rejected the notion that *IPXL* applies in the situation

present in this case and in *Oasis*:

> Defendants cite various cases holding that mixed apparatus and method claims are
> indefinite because it is unclear when infringement occurs. [citations omitted]
> However, these cases all deal with what appears to be an apparatus claim with
> method steps added into the claim. *See IPXL Holdings*, 430 F.3d at 1384 ("the
> system of claim 2 [including an input means] … and the user uses the input means
> …"); *In re Katz*, 639 F.3d at 1318 ("Katz's claim[s], however, create confusion as
> to when direct infringement occurs because they are directed both to systems and
> to actions performed by 'individual callers.'"); *Ariba, Inc.*, 2008 WL 3482521, at
> *8 ("A device operated by a potential seller is claimed, and the step in question is
> performed by a different computer, operated by a potential buyer, or the buyer's
> auctioneer."). ***Therefore, these cases do not apply to the argument advanced by***
> ***Defendants, because Claim 1 in the present case contains all method steps.***

Oasis, 2012 WL 602202 at *4 (emphasis added).

9.   The file history of the '150 Patent reflects that the so-called "mixed subject matter"

issue was never raised during prosecution. Two different USPTO examiners wrote detailed Office

Action notes, which included initial rejections of several of the Potentially Asserted Claims before

they were ultimately amended and allowed, and neither of them ever raised a single issue or

pointed out any problem with respect to the preamble of the claims or any "mixed subject matter"

concerns. The examiners' failure to raise a "mixed subject matter" issue was not because "mixed

subject matter" doctrine was unknown while the application that resulted in the '150 Patent was

being prosecuted. In fact, the early "mixed subject matter" case of *Ex parte Lyell*, 17 U.S.P.Q.2d

1548 (1990) was decided seven years before this application was filed in 1997. In addition, the

briefs of other CryptoPeak defendants show that "mixed subject matter" was included in the PTO's

Manual of Patent Examination Procedure ("MPEP") at least as early as 1999. (*See, e.g.,* Dkt. No.

18 in Case No. 2:15-cv-1288, at p. 3 n. 3.) Based on the file history, the examiners plainly were

not concerned about any "mixed subject matter" issue that would prevent issuance of the '150

Patent.

In any event, the file history is outside the pleadings, and no Moving Defendant has

attached it, so it is not before the Court and cannot be considered on the Motions to Dismiss. That

said, the file history is relevant to the issues raised by the Moving Defendants. Both the content

of the file history itself, and the fact that the Court cannot consider it here, are further reasons that

the Court should not grant the Motions to Dismiss.

10.   Finally, the Moving Defendants do not cite a single case where a court has

invalidated patent claims on "mixed subject matter" grounds on a Motion to Dismiss.

For all of these reasons, the Court should deny the Moving Defendants' Motions to Dismiss

on "mixed subject matter" grounds.

C.   The Motions to Dismiss on "Subject Matter Ineligibility" Grounds Should Be Denied Because the Potentially Asserted Claims Are Not Abstract Ideas But Instead Offer a Solution "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks" and Also Contain an Inventive Concept That Renders the Claims Subject Matter Eligible.

1.   Initial Observations

Before delving into the substance of the Moving Defendants' "subject matter ineligibility"

arguments, CryptoPeak offers a few initial observations:

●   Moving Defendants Sears and Yahoo go to great lengths to emphasize that

CryptoPeak has filed a total of 66 lawsuits based on the '150 Patent. Of the 29 defendant groups

in the First Wave Cases, <u>not one of them</u> saw fit to file a motion to dismiss on "subject matter ineligibility" grounds, despite the widespread prevalence of such motions in this District and across the country in the year-and-a-half since the Supreme Court's *Alice* decision. And this was not simply because most defendants settled or were dismissed early – <u>18</u> of the 29 defendant groups, represented by many of the biggest and most notable law firms in the country, answered or filed motions to dismiss on other grounds.

● Even in the Second Wave Cases, most of the defendants that appeared did not file motions to dismiss on "subject matter ineligibility" grounds. A total of 21 defendant groups (out of 37 Second Wave Cases) answered or filed motions to dismiss, and <u>only 7</u> of them raised "subject matter ineligibility" arguments. And even this number is somewhat overstated, because the "subject matter ineligibility" grounds are asserted by <u>only 3</u> law firms (the Webb firm and the Morgan Lewis firm each represent multiple defendant groups and filed identical motions on behalf of each of their respective clients).

● If "subject matter ineligibility" was a kill shot for the defendants in the CryptoPeak cases, it seems quite remarkable that 32 of 39 defendant groups appearing in the cases, including at least the first 18, would completely miss the issue and fail to raise it.

● Even among themselves, these Moving Defendants could not present unified, cohesive arguments. Each law firm took a decidedly different approach to try to squeeze the Potentially Asserted Claims of the '150 Patent into the "subject matter ineligibility" doctrine. For example, the defendants represented by the Webb firm hinge their arguments on a characterization of the claims at issue as a mathematical algorithm. *See, e.g.*, the Expedia Defendants' Motion to Dismiss, Dkt. No. 19 in the -1791 case, at p. 19 ("[T]he preamble of all five of the potentially asserted claims admits they are drawn to nothing more than an algorithm. The claims include

19

limitations directed only to mathematical algorithms … Claims 2, 3, 4, and 17 are similarly directed to generic mathematical formulations."). By contrast, the other Moving Defendants attempt to characterize the claims at issue as an abstract process for implementing cryptographic techniques using a general purpose computer. *See, e.g.*, the Ally Defendants' Motion to Dismiss, Dkt. No. 12 in the -1787 case, at pp. 8-9 ("[T]he claims describe a general abstract process built on the automation of previously known cryptographic techniques."); and the Sears Defendants' Motion to Dismiss, Dkt. No. 17 in the -1742 case, at p. 11 ("The Asserted Claims are likewise directed toward the patent-ineligible abstract concept of using a general-purpose computer to implement algorithms that generate, verify, and recover public and private keys.").

● Importantly, the Moving Defendants could not even agree – or even come particularly close to agreeing – on the purported "abstract idea" of the '150 Patent. Compare the three different formulations:

○ The Ally Defendants described the "abstract idea" as "generating, verifying, and recovering public and private keys by using software to implement long-known mathematical algorithms." *See* the Ally Defendants' Motion to Dismiss, Dkt. No. 12 in the -1787 case, at p. 2.

○ The Webb firm Defendants argued that the '150 Patent claims are directed to the "abstract idea" of "Performing a Mathematical Calculation." *See, e.g.*, the Expedia Defendants' Motion to Dismiss, Dkt. No. 19 in the -1791 case, at p. 18.

○ The Morgan Lewis Defendants argue that the "abstract idea" is "using algorithms to generate, verify, and recover public and private keys." *See, e.g.*, the Sears Defendants' Motion to Dismiss, Dkt. No. 17 in the -1742 case, at p. 10.[7]

---

[7] The Ally Defendants filed their Motion to Dismiss on January 28, the Webb Firm filed the earliest of its Motions to Dismiss on February 12, and Morgan Lewis filed its Motions to Dismiss on February 18.

Given that the Moving Defendants have the burden of articulating an "abstract idea" that squares with the actual claims at issue, *see, e.g., Ameranth, Inc. v. Genesis Gaming Solutions, Inc.*, 2014 WL 7012391 at **4-5 (C.D. Cal. Nov. 12, 2014) (Guilford, J.) (attached as Ex. E) (holding that defendants did not meet their burden of establishing the first step of the *Alice/Mayo* test because they failed to accurately articulate a proposed "abstract idea"), the failure of the Moving Defendants to agree on the purported "abstract idea" – and failure to even come particularly close to one another's attempts – suggests quite strongly at the very outset that the Moving Defendants' "subject matter ineligibility" arguments are not well-taken.

● In addition, the Moving Defendants' attempts at abstraction and their characterizations of the '150 Patent uniformly oversimplify the claims and miss (or obscure) the inventive concept and benefits of the invention of the '150 Patent. CryptoPeak will discuss the true nature of the patent and its benefits in more detail below.

2. Legal Standards for Subject Matter Eligibility Under 35 U.S.C. § 101

This Court is well familiar with the legal standards for subject matter eligibility under 35 U.S.C. § 101. *See, e.g., Genband US LLC v. Metaswitch Networks Corp.*, Case No. 2:14-cv-33, Slip Op. at pp. 3-5 (E.D. Tex. Jan 6, 2016); *Mobile Telecommunications Techs., LLC v. Leap Wireless Int'l, Inc.*, 2015 WL 5604691 at **1-2 (E.D. Tex. Sept. 23, 2015). Generally, the "subject matter eligibility" analysis consists of two steps. The first step concerns whether the patent claims at issue are directed to an "abstract idea." If not, the claims pass muster under § 101, and if so, the analysis proceeds to the second step. In the second step, the Court must determine if the elements

---

Therefore, the Webb Firm had the benefit of reading the Ally Defendants' motion before it filed on behalf of its clients, and Morgan Lewis had the benefit of reading both of the other firms' motions before it filed its clients' motions. Still, the Moving Defendants could not agree on the purported "abstract idea," and in fact consciously decided to present a different purported "abstract idea" than each defendant that had gone before them.

of the claim, individually, or as an ordered combination, contain an inventive concept that transforms the nature of the claim into a patent-eligible application. *See Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2355 (2014); *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1296-97 (2012).   In assessing subject matter eligibility, the Court must consider each claim as a whole, on a claim-by-claim basis. *See Diamond v. Diehr*, 450 U.S. 175, 188, 101 S. Ct. 1048, 1058-59 (1981).

Overlaid on this two-step analysis is the doctrine first articulated by the Federal Circuit in *DDR Holdings*, finding claims that are "necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks" to be subject matter eligible. *DDR Holdings*, 773 F.3d at 1257-59. The Federal Circuit in *DDR Holdings* was careful to distinguish such claims from those that broadly and generally claim use of the Internet to perform an abstract business practice, which are not subject matter eligible. *Id.* at 1258-59.

In addition, the Supreme Court has emphasized that the driving concern for subject matter ineligibility is preemption. *Alice*, 134 S. Ct. at 2354. Patents that do not pose a risk of preemption remain eligible for the monopoly granted under U.S. patent law. *Id.* at 2354-55. Courts recognize that the extent of preemption is an important factor in the section 101 analysis. *See, e.g., DDR Holdings*, 773 F.3d at 1259 ("the claims at issue do not attempt to preempt every application of the idea of increasing sales by making two web pages look the same … Rather, they recite a specific way to automate the creation of a composite web page by an 'outsource provider' that incorporates elements from multiple sources in order to solve a problem faced by websites on the Internet."). The extent of preemption may raise a fact issue that renders the granting of a motion to dismiss at the pleadings stage inappropriate. *See, e.g,, Presqriber, LLC v. AO Capital Partners*

LLC, Case No. 6:14-cv-440, Dkt. No. 125, Slip Op. at p. 11 (E.D. Tex. Mar. 31, 2015) (Mitchell, J.) (attached as Ex. F).

In motions to dismiss challenging the subject matter eligibility of a patent under the Rule 12(b)(6) standards, defendants "have the heightened burden of showing that the [patent's] subject matter is patent ineligible, after all inferences are drawn in favor of Plaintiff. *See Presqriber*, Slip Op. at 9. Although "under certain circumstances, a determination of patent validity under section 101 may be made at the pleading stage on a motion to dismiss, the issue of patentable subject matter requires a legal analysis that can – and often does – 'contain underlying factual issues.'" *Certified Measurement, LLC v. CenterPoint Energy Houston Electric LLC*, Case No. 2:14-cv-627, Dkt. No. 59, Slip Op. at p. 3 (E.D. Tex. Mar. 29, 2015) (Payne, J.) (attached as Ex. G) (quoting *Accenture Global Servs., GmbH v. Guidewire Software, Inc.*, 728 F.3d 1336, 1340-41 (Fed. Cir. 2013)). Cases may be dismissed only if the only plausible reading of the patent at issue is that there is clear and convincing evidence of invalidity on the grounds of subject matter ineligibility. *See, e.g., Rockstar Consortium US LP, Inc. v. Samsung Elecs. Co., Ltd.*, 2014 WL 1998053 at *3 (E.D. Tex. May 15, 2014) (Gilstrap, J.) (*analysis re-confirmed post-Alice in Rockstar Consortium US LP, Inc. v. Samsung Elecs. Co., Ltd.*, Case No. 2:13-cv-894, Dkt. No. 75 (E.D. Tex. July 21, 2014)) ("If there are factual disputes about the patent's claims, however, the question of patentable subject matter should be reserved until claim construction."). "While handling the issue of section 101 eligibility at the pleading stage is permissible, those issues are often inextricably tied to claim construction. Thus, it seems a definitive ruling on eligibility before claim construction is only warranted in narrow circumstances, making such a ruling the exception rather than the rule." *Id.* at pp. 3-4.

3. **The Potentially Asserted Claims of the '150 Patent Are Subject Matter Eligible Because They Are Not an Abstract Idea and They Contain an Inventive Concept**

The invention of the '150 Patent is in the field of cryptography. The invention relates to cryptosystems, and in particular to the escrowing and recovering of cryptographic keys and data encrypted under cryptographic keys. *See* '150 Patent, col. 1, lines 5-10. In the '150 Patent, the inventors solved an open problem that they identified as the "software key escrow" problem, by inventing an improved method to implement what they called an auto-recoverable and auto-certifiable cryptosystem. *See* Abstract of the '150 Patent; *see also* the inventors' related published article, "Auto-Recoverable Auto-Certifiable Cryptosystems" (attached as Ex. B; the "ARC Article") at p. 1. The invention of the '150 Patent overcame numerous limitations and shortcomings of the prior art.

The prior art and state of affairs that serves as the background to the invention of the '150 Patent is well-documented in the Patent. Prior to the '150 Patent, certain public key cryptosystems ("PKCs") allowed for encrypted, private communications over otherwise insecure channels, through the use of public and private encryption keys and key escrow systems involving the use of central trustees, or "trusted third parties" to register and escrow public keys. *Id.* at col. 1, lines 16-67. These "trustees" provided enhanced security for private communications over a network; however, all key escrow solutions known at the time of the invention of the '150 Patent suffered from some or all of the following disadvantages:

(a)   they required tamper-resistant implementation, or otherwise required hardware implementation, thereby imposing high implementation costs and slow establishment of use.

(b)   they required use of classified or otherwise proprietary algorithms, which may be unacceptable to persons skeptical about the escrow devices' security or operation.

24

(c)   to the extent implemented in software, they are subject to alteration.[8]

(d)   they required excessive protocol interaction in key generation and/or general use,

and in addition there may be only a small set of centralized trustee entities, thus resulting in

potential bottlenecks and delays.

(e)   they required excessive numbers of trusted third parties ("TTPs") to be involved in

system operation, thereby increasing the risk of security breaches and reducing scalability.

(f)   they required generation of cryptographic keys by the TTPs, so that a corrupt or

otherwise compromised TTP could put user security at risk by tampering with or disclosing a

user's keys.

(g)   they required the securing and management of database(s) of secret keys on behalf

of users.

(h)   they could be used by criminals to establish a shadow public key infrastructure,

thus defeating the purpose of the escrow system altogether.

See '150 Patent at col. 3, line 48, through col. 4, line 15; *see also* the complete Background section

of the '150 Patent at cols. 1-4 for a more complete description.

The invention of the '150 Patent solved these problems and represented a significant

advancement in secure communications using PKCs.   The invention eliminates the use of

"trustees" or TTPs and instead places the mechanics of the key escrow process in the hands of the

users (in terms of this case, the defendants), while maintaining the benefit of being able to provide

persons communicating with the users (in terms of this case, the clients of the defendants such as

persons using online banking or transacting e-commerce with the defendants) with verification

---

[8] The '150 Patent notes that this is an inherent problem of any software solution and not necessarily solved by the invention; however, the software in the invention is under the control of the user, not a third party, which may be considered by the user to be an advantage of the invention over prior art methods.

that their communications are secure and genuine. This is done via the methods set forth in the Potentially Asserted Claims of the '150 Patent. Using Claim 1 as an example, the user constructs a proof that public keys to be sent to clients were generated using a specific cryptographic algorithm, and this proof provides confidence to the clients that the public key was indeed generated properly by the user's specified algorithm. Claim 1 provides a very specific method by which this process occurs and provides the specific limitations and criteria that the method must meet. That is:

●   The proof must be a string of bits (that can be sent to the client), where the public availability of the string does not compromise the user's secret key; and

●   Constructing the proof requires access to the user's secret key; and

●   The proof must provide confidence to clients that the user's public key that was sent to the client was generated properly by the user's specified algorithm; and

●   Such confidence must be gained by the client without the client having access to the user's secret key.[9]

See the '150 Patent at col. 12, lines 24-41 (Claim 1). The other Potentially Asserted Claims are variations on this same technique.

The Moving Defendants gloss over and ignore these very specific requirements and limitations of the invention of the '150 Patent.

---

[9] Consider the alternative – the user could provide its secret/private key to the client, and the client could thereby use the secret key to verify that the communication was indeed genuine and from the user. This, however, would destroy the secrecy of the secret key. Instead, the '150 Patent describes the user providing the client a string of bits that can be publicly disclosed without compromising the secret key (rather than the secret key itself) but provides an equal amount of confidence to the client. The client's use of the user's public key to decrypt the communication from the user, along with the proof to provide confidence means that the system using this method is, as the inventors stated, "auto-recoverable" and "auto-certifiable."

26

The invention of the '150 Patent provides significant advantages over the prior art, as set forth in detail in the Patent:

(a)   the key escrow system using this method is software and can be distributed in source code form, easily, inexpensively, and with no loss of security.

(b)   [not applicable here]

(c)   the escrow system using this method requires the least amount of protocol interaction between parties that is theoretically possible.

(d)   only one private database is required to implement the escrow system, it may be kept private to prevent a shadow PKC from being established, and even if the database is exposed the users' private keys will not be exposed because the users have their own private keys.

(e)   the escrow system using this method allows the user's private key to be verified by anyone, and not just by a trusted authority (*i.e.*, "universal verifiability").

(f)   the escrow system using this method can be made shadow public key resistant, unlike prior art systems that could be abused to publish other PKC schemes.

See '150 Patent at col. 4, lines 18-59; *see also* the entirety of the ARC Article.

As the above discussion demonstrates, the claims of the '150 Patent, taken as a whole, describe a very specific invention. They are not abstract. They solved and/or improved upon a number of problems with the prior art and therefore contains inventive concepts. These claims are the quintessential "solution [that] is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." *DDR Holdings*, 773 F.3d at 1257.[10] And contrary to what the Moving Defendants would like to have the Court believe, (a) the '150 Patent does not claim cryptosystems or encrypted communications generally; (b) it

---

[10] Perhaps not surprisingly, none of the Moving Defendants ever cite or mention *DDR Holdings* in their Motions to Dismiss.

does not claim to cover prior art public key cryptosystems; (c) it does not constitute merely a mathematical algorithm; (d) it is not merely a computer-implemented method of an abstract idea or method that has been performed by humans for millennia.

Even beyond *DDR Holdings*, the relevant case law addressing the interplay between inventions in cryptology and subject matter eligibility strongly support CryptoPeak's position that the '150 Patent is subject matter eligible. For example, in *Loyalty Conversion Systems Corp. v. American Airlines, Inc.*, 66 F.Supp.3d 829 (E.D. Tex. 2014), Judge Bryson expressly noted that in the oral arguments in the Supreme Court in *Alice*, counsel for both the accused infringer and the Solicitor General pointed to patents on methods of encryption as examples of technology that are directed to "business methods" but would not be invalid as unpatentable subject matter. *Loyalty Conversion*, 66 F.Supp.3d at 846 n.7 ("[P]atents on methods for encrypting business transactions over the Internet … can involve complex algorithms that are designed to defeat even sophisticated efforts at decryption by hackers and other unauthorized persons.").

In another case where Judge Bryson sat by designation in this District, he expressly found that a cryptology-related method patent was subject matter eligible. *TQP Development, LLC v. Intuit Inc.*, 2014 WL 651935 (E.D. Tex. Feb. 19, 2014) (attached as Ex. H). There, Judge Bryson described the patent claims at issue as claiming:

> a method for transmitting encrypted data … by (1) inputting a seed value to identical pseudo-random number generators in the transmitter and receiver, (2) using the pseudo-random number generators to generate identical new key values at the transmitter and receiver, and (3) changing the key values … each time a predetermined number of blocks of data are transmitted.

Id. at *1. These limitations, Judge Bryson found, meant that the patent was "drawn to a very specific method of changing encryption keys" and therefore "it contains an 'inventive concept"

under the *CLS Bank* Federal Circuit precedent that the Supreme Court affirmed in *Alice*.[11] *Id.* at

*4.

      Similarly, in *Paone v. Mediatek USA, Inc.*, 2015 WL 4988279 (E.D.N.Y. Aug. 19, 2015)

(attached as Ex. I), the court found a patent claiming a computer-implemented method of

encrypting data to be subject matter eligible. There, the patent at issue described a particular form

of "block cipher," used for encoding digital information in groups, or "blocks," as opposed to one

at a time. *Id.* at *1 Even though computer-implemented block ciphers had been in wide use in the

United States long before the patent's application was filed, the court held that the specific

implementation described in the patent at issue was subject matter eligible. *Id.* at **1, 5-10. Like

the defendants in *Paone*, the Moving Defendants here "make no serious effort to explain why the

limitations recited by the ['150] patent fail to constitute an 'inventive concept,' much less why

they do not describe a 'very specific method of [providing secure communications with confidence

in an efficient manner.]"

      Finally, although CryptoPeak has already demonstrated above that the '150 Patent does not

preempt all uses of cryptology, or all public key cryptosystems, or even all methods of secure

communications over the Internet, CryptoPeak also notes that in practice companies use other

methods of establishing secure, trusted communications over the Internet and other networks,

including for purposes such as online banking and e-commerce transactions. As one example,

aside from the ECC cipher suites for TLS protocol that Cryptopeak accuses, even the Moving

---

[11] Judge Bryson also made clear that the machine-or-transformation test has absolutely no application to patents in the field of cryptology. *TQP Development*, 2014 WL 651935 at *5 ("In the case of an invention in the field of encryption … the entire object of the invention is to transform data from one form into another…. In that setting, it does not make sense to say that the transformation of data … cannot qualify as a patent-eligible invention, because that is what the field of cryptology is all about.").

Defendants also use a protocol known as RSA,[12] when ECC cipher suites for TLS are not available. There are many companies other than those who are defendants in the CryptoPeak cases that do not utilize ECC cipher suites for TLS at all. Because this is a motion to dismiss, CryptoPeak is unable to present evidence on this point; however, CryptoPeak wishes to advise the Court that it could present evidence on this point if it was appropriate to do so.

For all of these reasons, the Court should deny the Moving Defendants' Motions to Dismiss on "subject matter eligibility" grounds.

<div align="center">

CONCLUSION

</div>

For the reasons set forth herein, Plaintiff CryptoPeak respectfully requests that the Court deny the Motions to Dismiss and grant CryptoPeak such other and further relief to which it is entitled.

Dated: March 3, 2016   Respectfully submitted,

                                                     /s/ Craig Tadlock
                                                     Craig Tadlock
                                                     State Bar No. 00791766
                                                     John J. Harvey, Jr.
                                                     State Bar No. 09179770
                                                     Keith Smiley
                                                     State Bar No. 24067869
                                                     TADLOCK LAW FIRM PLLC
                                                     2701 Dallas Parkway, Suite 360
                                                     Plano, Texas 75093
                                                     903-730-6789
                                                     craig@tadlocklawfirm.com
                                                     john@tadlocklawfirm.com
                                                     keith@tadlocklawfirm.com

                                                     Attorneys for Plaintiff
                                                     CryptoPeak Solutions, LLC

---

[12] CryptoPeak asserts, however, that RSA is not an acceptable non-infringing alternative, because it is less secure than ECC cipher suites for TLS in meaningful ways, and is in other ways less desirable.

CERTIFICATE OF SERVICE

The undersigned certifies that a copy of the foregoing was served on all parties who have appeared in this case on March 3, 2016, via the Court's CM/ECF system, pursuant to Local Rule CV-5(a)(3).

 /s/ Craig Tadlock
Craig Tadlock